

平成 25～26 年度地域医療連携の普及に向けた 健康情報活用基盤実証事業

緊急時、災害時、障害時の対応手順

Ver.1.1

平成 26 年 8 月 22 日

公益社団法人 石川県医師会

目次

1. 目的	3
2. 適用範囲	3
3. 責任と権限	4
3. 1 責任と権限	4
3. 2 権限の委譲	4
4. 緊急時の対応	5
4. 1 緊急時の考え方	5
4. 2 緊急時の対応方法	5
4. 3 アクセス履歴の保存	5
5. 災害時の対応	6
5. 1 災害発生 of 判断基準	6
5. 2 災害のフェーズ分け	6
5. 3 災害時の対応方法	7
5. 4 アクセス履歴の保存	7
6. 障害時の対応	8
6. 1 障害レベルの分類	8
6. 2 障害時の対応方法	9
7. 原因の究明と再発防止対策	9
8. 障害等の公表	9
9. 教育と訓練	9
10. 対応手順の見直し	9

1. 目的

本対応手順は、平成 25～26 年度地域医療連携の普及に向けた健康情報活用基盤実証事業（以下「本事業」という。）に係わる実証システム（以下「本システム」という。）の運用管理規程に定める「緊急時、災害時、障害時の対応手順」に関するもので、緊急時、災害時、障害時においてサービスの提供、運用と業務の混乱を防止するため円滑な対処を行えるよう、その手順を定めることを目的とする。

なお、本対応手順は本システムの運用範囲における取り決めであって、本対応手順の範疇を超える大規模な激甚災害等が発生した場合は、各参加機関が定める事業継続計画や政府、行政機関の定める各種法令や指示を優先するものとする。

2. 適用範囲

本事業および本対応手順で想定する場面を表 1 に示す。

表 1 本事業および本対応手順で想定する場面

分類	考え方	例
緊急	患者の意識が無い状態	患者の意識が無い状態で参加機関に救急搬送された場合
災害	石川県地域防災計画に基づき、災害対策本部が設置された場合	石川県下に震度 5 強（5+）が発生したため、知事が災害対策本部を設置した場合
障害	本システムの障害、個人情報の漏えい・滅失・棄損に関する事件・事故	ネットワーク機器の故障により本システムが利用不可となった場合

3. 責任と権限

3.1 責任と権限

- (1) 事業管理者
本事業の運営に関する管理責任を負う。
- (2) 事業実施責任者
本事業の運営に係わる実施責任を負う。
- (3) 運用管理責任者
本システムに係わる障害、事故等の全責任を負い、事業管理者、事業実施責任者への報告責任、原因の究明、復旧の措置、再発防止の対策等の管理責任を負う。
- (4) システム管理者
運用管理責任者の指示の下に、障害、事故等の原因究明、復旧措置、再発防止措置の実施責任を負う。
- (5) リモート保守責任者
システム管理者の指示の下に、本システムが適切に稼働するよう維持、管理、保守を行う責任を負う。
- (6) サポートセンター責任者
本システムで、システム管理者の指示の下に、障害、事故等の苦情相談窓口、サービス提供者、システムベンダー等との連絡調整の実施責任を負う。

3.2 権限の委譲

以下の考え方に基づいて権限の委譲を行うものとする。

- (1) 「3.1 責任と権限」に示す者が当該責任の範囲での指揮をとることができない場合には、同一組織内の従事者に権限を委譲することができるものとする。
- (2) 権限を委譲する際の判断基準、委譲を指示する者、権限の委譲を解除する基準等については、各組織の規定にしたがうこととする。(同一組織に置いて、より上位の役職の者が、業務を代行することがある。)

4. 緊急時の対応

4.1 緊急時の考え方

本事業においては、以下の場면을想定する。

- (1) 患者の意識が無い状態で救急搬送され、患者が IC カードを提示できない場面

4.2 緊急時の対応方法

- (1) 患者の意識が無い状態で救急搬送され、患者が IC カードを提示できない場面
医師・歯科医師・薬剤師・看護師・管理栄養士は HPKI カードを用いて本システムへログインした後、「緊急時・災害時ボタン」を押下することにより、当該患者の情報を氏名等で検索した上で、閲覧を行う。

4.3 アクセス履歴の保存

「4.2 緊急時の対応方法」をとった場合には、患者の情報を参照したことをログとして残すとともに、患者自身が確認可能な状態とする。

5. 災害時の対応

5.1 災害発生の判断基準

災害発生の判断基準として、石川県地域防災計画に基づいた県知事の判断を用いることとする。具体的には、石川県地域防災計画に基づき、災害対策本部が設置されたことをもって、災害時の対応を開始する。

5.2 災害のフェーズ分け

表 2 に示す通り、災害のフェーズによって必要となる対応は異なるが、本事業では、ネットワークインフラが利用可能となるフェーズ（業務再開フェーズ）を想定した対応を取ることとする。

災害発生から 1 カ月以降は 2 週間毎に、通常のアクセス管理の運用に戻すかどうかの判断を行うものとする。

なお、業務再開、業務回復フェーズから全面復旧フェーズへの切り換えは、事業管理者の判断により行う。

表 2 災害のフェーズ分け

フェーズ ¹ (時間経過)	概要	備考
BCP 実行フェーズ (発生直後から 72 時間)	ネットワークインフラが被害を受けていると想定し、ネットワークから切り離したスタンドアロンでの使用や、紙での運用等が考えられる。	本事業ではこの部分のシステム構築は対象外とする。
業務再開フェーズ 業務回復フェーズ (72 時間から 1 カ月) ※本事業で対応する部分	ネットワークインフラが利用可能となるフェーズを想定。通常時の運用に戻す前段階として、一定のアクセス制限を設けることが想定される。	本事業では、本フェーズで利用する機能について検討し、実装する。
全面復旧フェーズ (1 カ月以降)	定期的 (2 週間ごと) に、通常のアクセス管理の運用に戻すかどうかの判断を行う。	通常運用に戻していくことになる。運用ルールを整理する。

¹ 厚生労働省 「医療情報システムの安全管理に関するガイドライン 第 4.2 版」
6.10 災害等の非常時の対応 の内容を参考に記載。

5.3 災害時の対応方法

災害時には、ネットワークインフラが復旧する段階（発災から 72 時間程度経過後を目安とする）で、災害時のアクセス権管理でシステムが利用可能となるような対応を行う。

(1) システム利用者の認証

本事業では、医師・歯科医師・薬剤師・看護師・管理栄養士は HPKI カードを用いて本システムへログインすることとしているが、災害時運用においては、認証を通過させる方式をとる。認証を通過させるためには、本システムに接続する端末に設定をする必要があり、設定に必要なファイル群については、災害時に CD 等で配布（使用可能な PC がある場合）、あるいはセットアップ済みの PC を配布することとする。また、災害時に本システムを利用する際には、利用者の氏名・住所のほか、指紋を採取、保管することとし、不正利用等があった場合に利用者の特定に使用するものとする。

(2) 患者情報の開示

「緊急時・災害時ボタン」を押下することにより、当該患者の情報を氏名等で検索した上で、閲覧を行う。

5.4 アクセス履歴の保存

「5.3 災害時の対応方法」をとった場合には、患者の情報を参照したことをログとして残すとともに、患者自身が確認可能な状態とする。

6. 障害時の対応

6.1 障害レベルの分類

障害内容によりレベル0からレベル4の5つに分類し、迅速かつ適切な対応を図る。表3に障害レベルと障害内容、対処決定方法等を示す。

表3 障害レベルと障害内容、対処決定方法等

障害レベル	インフラ障害等	システム障害等			個別障害
	レベル4	レベル3	レベル2	レベル1	レベル0
頻度	極めてまれ		まれ		有り
障害内容	(1)地域のネットワーク障害 (2)データセンターの被災 (3)参加医療機関の建物・人への被災 (4)地域の患者の被災、その他	データセンター、バックアップセンターの障害(ネットワーク障害、システム障害、電源障害、空調機障害等)	(1)一部のネットワーク障害 (2)一部のサービス障害 (3)一部の医療機関のシステム障害 (4)その他		(1)システムを構成する端末等の障害 (2)個別の医療機関のネットワーク障害又は操作上の問題 (3)その他
主な事象	(1)人命に係わる事象 (2)地域のネットワーク、連絡網に影響 (3)サービスの全面停止(長期停止の可能性)	(1)サービスの停止又は一部サービスの停止 (2)短期・中期のサービス停止	(1)一部の利用者の利用ができなくなる。 (2)一部のサービスの利用ができなくなる。 (計画保守での停止を除く)		個々の障害に応じて異なる。
復旧までの期間見通し	長い、予測が困難	1日以上の見込み	2時間以上、1日以内の見込み	2時間以内の見込み	個々の障害に応じて異なる。
対処方針の決定	(1)事業管理者もしくは事業実施責任者にて判断 (2)連絡手段の確保が困難な場合又は緊急措置を講じる必要がある場合は、運用管理責任者で判断	(1)事業実施責任者もしくは運用管理責任者にて判断 (2)運用管理責任者は、事業管理者、事業実施責任者に対処の結果を報告する。	(1)事業実施責任者もしくはシステム管理者にて判断 (2)システム管理者は、対処の結果を運用管理責任者に報告する。	(1)運用管理責任者もしくはシステム管理者にて判断 (2)システム管理者は、対処の結果を運用管理責任者に報告する。	(1)データセンター、ネットワーク、リモート保守責任者もしくはサポートセンター責任者にて判断 (2)データセンター、ネットワーク、リモート保守責任者もしくはサポートセンター責任者は、システム管理者に対処の結果を報告する。

6.2 障害時の対応方法

障害発生後は、表 3 により各障害レベルで定められた責任者（「対処方針の決定（1）」に記載の者）の判断の元で、迅速かつ適切な復旧を行う。その手順を以下に示す。

(1) 対処方針の決定

責任者は、障害に関する情報収集を行い、復旧に向けた対処方針を決定する。

(2) 現場での作業委託

責任者は関連ベンダの招集を行い、関連ベンダへ現場での復旧作業を委託する。

(3) 適切なタイミングでの報告

責任者は、対処の状況もしくは結果を、適切なタイミングで現場より報告させる。当初見込みより復旧まで時間がかかる、もしくは復旧の見込みが立たない場合、責任者は以下のいずれかの対応を行う。

- ・ 対処方針の見直し
- ・ 上位障害レベルの責任者へのエスカレーション

(4) 上位責任者への報告

責任者は、対処の結果を上位の責任者に報告する。

7. 原因の究明と再発防止対策

(1) システム管理者は、障害の発生原因を究明する。

(2) システム管理者は、再発の防止策を事業実施責任者および運用管理責任者に報告し、防止策を実施する。

(3) 重大な障害等の場合には、事業実施責任者もしくは運用管理責任者は、事業管理者に報告する。

8. 障害等の公表

事業実施責任者は、障害の重大さに応じて、その内容、原因、対処の結果等を事業管理者と協議し、事業管理者は必要と判断される場合には外部に公表する。

9. 教育と訓練

事業実施責任者もしくは運用管理責任者は、障害、災害の発生に備えて、定期的にシステム管理者、データセンター、ネットワーク、リモート保守責任者、サポートセンター責任者等の教育と訓練を行うものとする。

10. 対応手順の見直し

事業管理者は、運用状況等に問題がある場合には、本対応手順を見直すことができるものとする。

以上